Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 74 – 83 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CHALLENGES AND OPPORTUNITIES OF AI-DRIVEN CYBERSECURITY FOR SMALL AND MEDIUM ENTERPRISES (SMES) TOWARDS POVERTY REDUCTION IN NIGERIA

Ayepeku Olukayode FELIX[1], Olofinlade Samuel OLUWAPELUMI[2]

[1]Department of Mathematical and Computing Science, Thomas Adewumi University Oko-Irese, Kwara State, Nigeria
[2]University of Ilorin, Department of Accounting and Finance, Ilorin, Kwara State, Nigeria

ABSTRACT: Nigerian Small and Medium Enterprises (SMEs) face significant challenges in protecting their digital assets due to the increasing proliferation of cyber threats which tends to affect their goals of intermediary in employment generation towards reducing poverty in the society. This article examines the role of artificial intelligence (AI) in reducing risks and opening new opportunities for the SMEs in safeguarding their assets towards job creation which is an agent of fighting poverty to actualise SDGs. Limited resources, financial constraints, and a lack of awareness about cybersecurity risks contribute to the challenges faced by SMEs. However, the integration of AI-driven cybersecurity solutions offers significant opportunities. AI enhances threat detection capabilities, providing real-time analysis and rapid response mechanisms. Automation of routine tasks reduces the burden on limited resources and ensures a more proactive approach to cyber defence. AI solutions tailored for SMEs offer cost-effective options to bolster their cybersecurity posture. The article delves into case studies of successful implementation of AI-driven cybersecurity measures and explores government initiatives and support programs aimed at assisting SMEs in adopting these technologies. Collaborative approaches, information sharing, and employee training are crucial best practices for SMEs in navigating the evolving threat landscape. The article concludes by discussing emerging trends in AI-driven cybersecurity for SMEs and emphasizing their pivotal role in fostering sustainable business growth and resilience against cyber threats in Nigeria.

KEYWORDS: AI, AI-Driven, Cybersecurity, Enterprises, SMEs, Small, Medium, Poverty reduction, JEL Classification: G 21, G33.

1. INTRODUCTION

Cybersecurity faces an ever-evolving landscape of threats, including sophisticated malware, ransomware attacks, and vulnerabilities in software and networks. Artificial Intelligence (AI) has emerged as a powerful tool in enhancing cybersecurity capabilities, offering advanced features for threat detection, response, and mitigation. However, Nigeria's Small and Medium Enterprises (SMEs) are not left out of the threats as the SMEs tailored objective of provision of small assistance for economic growth are grappling with a mounting wave of cyber threats that pose significant risks to their operations and overall cybersecurity resilience towards the attainment of their objectives. This comprehensive exploration delves into the evolving threat landscape, highlighting the specific challenges faced by SMEs in Nigeria. Small and Medium-sized Enterprises (SMEs) are increasingly becoming targets for cyber-attacks due to several factors. These attacks can have severe consequences for these businesses, ranging from financial losses to reputational damage and the attainment of SDGs goal tend not to be actualised, and high poverty rates persist in many target states in the countries. As a result, in 2015, ending poverty (measured by people living on less than $1.20 per day) became the top precedence of the United Nations member states' global Sustainable Development Goals (SDGs) 2030 agenda. The global objectives of the United Nations aimed to end poverty and shield the planet by 2030. Sadly, the COVID-19 global pandemic has left substantial evidence of inevitable future poverty growth with the threat of financial and technological challenges. These cyber-attacks, often characterized by advanced persistent threats (APTs), exploit vulnerabilities in SMEs' networks and systems. (Ibitamuno 2023). The World Economic Forum's Global Risks Report points to the growing concern of supply chain vulnerabilities for Nigerian businesses. SMEs, often interconnected within extensive supply chains, are increasingly susceptible to attacks targeting third-party suppliers, which can result in significant disruptions. (“World Economic Forum: Global Risks Report 2019” 2019). A recent survey in Nigeria highlights a

concerning lack of cybersecurity awareness among employees of SMEs. This knowledge gap contributes to the success of various cyber-attacks, including those leveraging social engineering and insider threats, emphasizing the need for targeted awareness programs. ("Cybersecurity, Privacy, and Data Protection: State of the Art in Iran, Nigeria, Portugal, and the USA." 2023).

AI technologies, such as machine learning (ML) and deep learning, enable cybersecurity systems to analyze vast amounts of data rapidly. By learning from historical patterns and anomalies, AI-driven systems can identify potential threats that may go unnoticed by traditional signature-based methods. Real-time threat detection and prevention are critical components in safeguarding systems and networks from evolving cyber threats. (Maurya 2023). AI-driven cybersecurity solutions excel in behavioral analysis, allowing them to understand normal user behavior and identify deviations that may indicate a security threat. This proactive approach helps in early detection of anomalous activities, reducing the time it takes to respond to potential breaches. (Deepshikha Aggarwal, Deepti Sharma, Archana B. Saxena**,** 2023). AI-powered automation streamlines the response to security incidents. It enables rapid decision-making and executes predefined responses to mitigate threats. This is particularly crucial in dealing with fast-spreading malware and minimizing the impact of cyberattacks. (Tonhauser and Ristvej 2023). AI-driven cybersecurity solutions have the capacity to adapt and evolve based on new threat intelligence. Machine learning algorithms continuously learn from new data, allowing them to improve their accuracy over time. This self-learning capability enhances the resilience of cybersecurity systems against emerging threats. (Gheibi, Weyns, and Quin 2020)

2. CHALLENGES FOR SMES IN NIGERIA

The growing inclination of poverty is an exceptionally long-standing problem particularly in the North eastern regions of Nigeria which is prone to different security breach, many people as many people live below the poverty line and this poverty level continues to increase. Food and nutritional insufficiencies have reached a monumental proportion with malnourishment causes underweight in infants is a bane to attainment of SMEs goals. The multiplier effect of this bane on Small and Medium-sized Enterprises (SMEs) in Nigeria is part of numerous faces of challenges, and one significant hurdle is the limited availability of resources, particularly financial constraints. This challenge prevents SMEs from investing in advanced cybersecurity measures.

SMEs in Nigeria often operate within tight budgets, allocating resources to various aspects of their business operations. Limited financial resources present a significant challenge when it comes to addressing the complex and evolving landscape of cybersecurity threats. It is often said that people in rural areas have ideas but no financial inclusion is essential to drive the micro and macroeconomics factors towards growth and development which is part of the objectives of SMEs. Investing the little available funds in advanced cybersecurity measures requires a substantial financial commitment which the SMEs does not have in excess. SMEs, constrained by paucity of fund and essential financial resources referencing budgetary limitations, may find it challenging to allocate sufficient funds to implement robust cybersecurity infrastructure and technologies. (Anuj Thapliyal, 2022). A cybersecurity system that is out of date due to a lack of funding may expose SMEs to sophisticated cyberattacks. Sensitive consumer and corporate data may be in danger due to this low investment's insufficient defense against cyberattacks. SMEs that do not invest enough in cybersecurity solutions are more vulnerable to ransomware, phishing, and data breaches, among other cyberthreats. There might be serious interruptions to corporate operations if there are insufficient protection systems. (Kariuki, Ofusori, and Subramaniam, 2023).

Inadequate cybersecurity measures expose SMEs to potential reputational damage and regulatory penalties. Data breaches and cyber incidents can erode customer trust, impacting the company's reputation and potentially leading to legal consequences. According to a survey conducted by Ugwuja, V. C., Ekunwe, P. A., & Henri-Ukoha, A. (2020), a significant percentage of SMEs in Nigeria lack a comprehensive understanding of cybersecurity risks. SMEs often face challenges due to limited investment in training their employees on cybersecurity best practices. A study by Benz

and Chatterjee (2020) highlighted that only 40% of SMEs provide regular cybersecurity training to their staff. SMEs may struggle with understanding and complying with cybersecurity regulations. Marotta and Madnick 2020 emphasized the need for simplified guidelines and increased support for SMEs to navigate and adhere to cybersecurity regulations. Failure can lead to increased risk of cyber-attacks, data breaches, loss of sensitive information, financial losses, identity theft and fraud, reputation damage, the spread of malicious software, and weakened national security, to mention but a few. Insufficient awareness of available AI-driven solutions in cybersecurity is a significant challenge, impacting the ability of organizations to defend against evolving cyber threats. AI is instrumental in enhancing cybersecurity detection of sophisticated threats, real-time incident response, and automation of routine tasks. Moreover, lack of education and training also contributes to a gap in understanding among employees and decision-makers. Misconceptions and overreliance on AI can lead to unrealistic expectations and potential oversights in cybersecurity strategy. Global variations in awareness levels vary across regions, with more technologically advanced regions generally being more informed. The awareness of AI-driven cybersecurity solutions varies across different industries, regions, and organizational sizes. Large enterprises and tech-savvy industries generally exhibit higher levels of awareness, as they are more likely to invest in cutting-edge cybersecurity measures.

Cybersecurity professionals are well-informed about the capabilities and potential of AI-driven solutions, and increased media coverage and industry reports have contributed to greater awareness. However, SMEs and non-technical industries often lag in awareness due to limited resources, budget constraints, and a lack of dedicated IT personnel. According to (Bada & Nurse, 2019) SMEs in Nigeria often lack awareness and education about cybersecurity, leading to a lack of understanding of potential risks and consequences of cyber threats. This lack of awareness can increase their vulnerability to social engineering attacks and other cyber threats. Regional disparities and regulatory influence also play a role in fostering awareness about AI-driven solutions. The future outlook for AI-driven cybersecurity is expected to see rising interest and investments due to the ongoing rise in cyber threats and the recognition of AI's potential. Education and training initiatives will contribute to increased awareness, and the integration of AI tools and solutions into mainstream operations will expose a broader audience to its capabilities and benefits. Many Nigerian SMEs face financial constraints, hindering their ability to invest in robust cybersecurity measures. This insufficient budget makes them more susceptible to cyber threats, affecting their overall security. (Joseph, Obikaonu, Ariolu, Nwolisa, & Aderohunmu, 2021). Many Nigerian SMEs lack the latest cybersecurity technologies due to outdated IT infrastructure and lack of technology adoption. This vulnerability leaves them vulnerable to cybercriminals, as they may not have the latest security patches or defenses against evolving threats. (Reference: Oluwaseyi, J. O., & Afolayan, A. M. (2020). "Challenges of IT Infrastructure in Nigerian SMEs." International Journal of Computer Applications, 182(18), 43-48.) Nigerian SMEs face challenges in recruiting and retaining skilled cybersecurity professionals due to competition with larger enterprises. This shortage leaves them without the expertise to develop and maintain effective cybersecurity strategies, increasing their vulnerability to attacks. (Kassar, 2023). Nigerian SMEs face regulatory compliance challenges in cybersecurity, potentially leading to legal consequences and reputational damage. Clear and accessible guidelines are crucial to address these challenges and ensure compliance for SMEs. (Ukwuoma, Williams, & Choji, 2022)

3. OPPORTUNITIES PRESENTED BY AI-DRIVEN CYBERSECURITY

This paper discusses the potential of AI-driven cybersecurity for Small and Medium Enterprises (SMEs) in Nigeria towards poverty reduction. AI-driven cybersecurity solutions can automate threat detection and response, reducing response times and enhancing the speed of response.

Predictive analytics can also be used for proactive defence, allowing SMEs to implement pre-emptive measures before they escalate into major security incidents that can have negative impact of food security thereby enhancing poverty alleviation. AI-driven cybersecurity solutions can be customized to suit the specific needs and scale of SMEs, offering flexibility and scalability. Behavioural biometrics, facial recognition, and anomaly detection algorithms can enhance user authentication and access control, reducing the risk of unauthorized access. (Gaggero, Girdinio, & Marchese, 2021)

AI-driven cybersecurity solutions can also be cost-effective through resource optimization. Automated threat detection and response mechanisms reduce the need for extensive human intervention, allowing SMEs to allocate resources efficiently. This cost-effectiveness enhances the affordability of advanced cybersecurity measures and makes it an attractive option for SMEs in Nigeria. Overall, AI-driven cybersecurity offers a promising solution for SMEs in the digital age. (Bhardwaj & Kaushik, 2022)

Artificial Intelligence (AI) is revolutionizing cybersecurity by enhancing threat detection capabilities through advanced analytics, automation, and machine learning. AI algorithms can detect anomalies by establishing a baseline of normal behaviour, while behavioural analysis allows AI to analyse user and entity behaviour to identify deviations from typical patterns. Machine learning models enable AI to analyse vast amounts of data, improving accuracy in identifying known and unknown threats. AI can integrate threat intelligence feeds and databases to stay updated on the latest known threats, reducing the time to detect and respond to emerging threats. (Alfayoumi, Eltazi, & Elgammal, 2023). Predictive analysis allows AI to predict potential threats based on historical data and ongoing trends, allowing organizations to proactively address emerging threats before they escalate. AI-driven automation can handle routine security tasks, freeing up human resources to focus on more complex threat analysis and response. Deep learning for image and speech recognition enhances detection capabilities in areas like video surveillance and voice command systems. Dynamic threat modelling allows AI to dynamically model evolving threats based on real-time data, providing a more accurate and adaptive threat detection system. (El- El-Sofany, 2022)

AI plays a crucial role in various aspects of cybersecurity, including threat detection, log analysis, incident triage, vulnerability assessment, and phishing detection which the SMEs can benefit from in attending to its pivotal goals. AI-powered tools process and correlate logs from multiple sources to identify anomalies and potential security events, while automated incident response platforms triage incidents, prioritize critical ones, and provide comprehensive reports on potential vulnerabilities. To make AI solutions scalable and affordable for Small and Medium Enterprises (SMEs), a strategic approach considering resource constraints, cost-effectiveness, and specific requirements is needed. Strategies include using cloud-based AI services and platforms, leveraging open source AI tools, choosing modular and customizable solutions, exploring pre-built AI solutions, prioritizing AI applications that align with core business objectives, adopting AI as a Service (AIaaS), incremental implementation, employee training and upskilling, low-code/no-code platforms, regular evaluation and optimization, and exploring government initiatives and grants.

Artificial Intelligence (AI) is revolutionizing cybersecurity for Nigerian Small and Medium Enterprises (SMEs) by enabling real-time analysis of patterns and anomalies. AI-powered systems monitor network activities, user behaviours, and system logs, identifying potential threats as they emerge. It excels in pattern recognition, allowing it to distinguish normal behaviour from anomalies. AI can also help mitigate zero-day threats by recognizing patterns associated with previously unseen threats. AI-driven solutions conduct behavioural analysis for insider threats, raising alerts in case of suspicious behaviour. These solutions are scalable and affordable, contributing to regulatory compliance requirements in industries with stringent data protection and privacy regulations. (Rizvi, 2023). The integration of Artificial Intelligence (AI) in automated incident response systems offers Nigerian SMEs a significant opportunity on innovative financial

programmes and reforms that can support entrepreneur financing poverty reduction mechanism. AI-driven systems enable real-time threat mitigation, allowing for immediate identification and mitigation of cyber threats. This is particularly beneficial for SMEs in Nigeria, where speed of response minimizes the impact of security incidents. AI algorithms analyse incoming threat data in real-time, aligning incident response strategies with the latest threat landscape. This reduces response time, reducing damage and disruptions. AI systems also learn from past incidents, adapting response strategies over time. Continuous monitoring and analysis of network activities further enhance the effectiveness of AI-powered systems. (Chahal, 2023)

The digital age presents significant opportunities for Small and Medium Enterprises (SMEs) in Nigeria, particularly when leveraging AI-driven cybersecurity solutions. Key opportunities include proactive threat detection and prevention, cost-effective security measures, tailored solutions, enhanced incident response capabilities, government support and incentives, global competitiveness, cybersecurity skills development, data privacy and compliance, innovation and digital transformation, collaborative threat intelligence sharing, business resilience and continuity, customizable training programs, market differentiation, and ecosystem collaboration. Proactive threat detection and prevention enable SMEs to identify patterns indicative of potential attacks and take preventive measures, reducing the risk of data breaches. Cost-effective security measures reduce the need for extensive human intervention, allowing SMEs to enhance their cybersecurity posture without significant resource investments. Tailored solutions for SMEs address their unique needs and challenges, while automated incident response minimizes the impact of security breaches, reducing downtime and potential financial losses. Governments and regulatory bodies may offer support and incentives for SMEs adopting AI-driven cybersecurity measures, making advanced technologies more accessible. Implementing AI-driven cybersecurity can enhance global competitiveness, build trust with international partners and customers, and improve cybersecurity skills development among the workforce. AI can also aid SMEs in ensuring data privacy and compliance with regulatory requirements, building a reputation for secure and compliant operations.

AI-driven cybersecurity aligns with the broader trends of innovation and digital transformation, attracting customers who prioritize security in their partnerships. Collaborative threat intelligence sharing among SMEs and within industry networks benefits SMEs from shared insights, collective defence mechanisms, and a collaborative approach to combating cyber threats. Customizable training programs for SMEs enhance the overall security culture and help SMEs differentiate themselves in the market. Ecosystem collaboration within the cybersecurity ecosystem, including partnerships with service providers, strengthens SMEs' overall cybersecurity defences.

4. CASE STUDIES

AI-driven cybersecurity measures are increasingly being adopted by SMEs worldwide to improve their security posture for risk reduction. These solutions offer benefits such as real-time threat detection, endpoint protection, user and entity behavioural analytics (UEBA), automated incident response, cloud security, phishing detection, network traffic analysis, and security orchestration and automation response (SOAR). In Nigeria, AI-driven cybersecurity has shown potential positive impacts on SMEs business operations, including improved threat detection, endpoint protection, proactive insider threat detection, cloud security enhancement, phishing prevention, efficient network traffic analysis, and enhanced data privacy and compliance. However, the outcomes may vary depending on the specific context and implementation of AI-driven cybersecurity solutions. The e-commerce industry in Nigeria faces challenges and different risk such as business model risk, operational costs, and user disposable income. However, the market is rapidly growing, projected to reach $75 billion by 2025 and $120 billion by 2030. This growth is driven by factors such as the growing youthful population, increasing internet penetration in rural areas, rising disposable

incomes, and a growing middle class. The market's success depends on overcoming these challenges and leveraging Nigeria's FX reserve and economic growth through maintaining appropriate levels of investment, particularly in infrastructure This is crucial to attaining this aim of job opportunities, employment growth which should be made available for the youth through small and medium business towards self-reliant and be an employer of labour from their small-scale enterprises with their entrepreneur innovative efforts and lots more which the AI can safeguard

5. GOVERNMENT INITIATIVES AND SUPPORT

The Nigerian government has implemented several initiatives to support SMEs in enhancing their cybersecurity. These include the National Cybersecurity Policy and Strategy, which aims to create a secure cyberspace for individuals and businesses, and guidelines issued by the National Information Technology Development Agency (NITDA) on data protection. The government has also initiated capacity building programs to enhance SMEs' cybersecurity skills through training sessions, workshops, and seminars towards reducing the cyber security challenges and business systematic and unsystematic risk which is a bane to Nigeria business environment. Opportunities for AI-driven cybersecurity in SMEs include automation and threat detection, collaborative initiatives between SMEs and government agencies, and incentives for adoption. These can help mitigate the challenges posed by limited resources and promote the adoption of advanced protective measures. Additionally, the government can introduce tax breaks or grants to encourage SMEs to invest in AI-driven cybersecurity solutions, alleviating budget constraints and promoting the adoption of advanced protective measures. Government initiatives to promote cybersecurity in Small and Medium Enterprises (SMEs) are crucial for ensuring the resilience of the national cybersecurity landscape. These initiatives include cybersecurity awareness campaigns, training and capacity building programs, access to cybersecurity resources, incident response support, regulatory compliance assistance, financial support and grants, information sharing platforms, national cybersecurity standards for SMEs, public-private partnerships, cybersecurity insurance awareness, and international collaboration.

These initiatives aim to increase awareness among SMEs about cybersecurity threats and best practices, provide affordable access to cybersecurity tools and resources, assist SMEs in responding to and recovering from cyber incidents, and help them understand and comply with cybersecurity regulations. Financial support and grants are also offered to SMEs for investing in cybersecurity infrastructure, training, and technology. Information sharing platforms facilitate the exchange of cybersecurity threat intelligence among SMEs, while national cybersecurity standards are defined and disseminated. Public-private partnerships foster collaboration between government agencies, industry associations, and SMEs to discuss cybersecurity challenges and solutions. Cybersecurity insurance awareness encourages SMEs to consider it as part of their risk management strategy. International collaboration facilitates international cooperation on cybersecurity matters affecting SMEs.

AI-driven cybersecurity measures can be challenging for small and medium-sized enterprises (SMEs) due to resource constraints. Governments, industry bodies, and other organizations offer support programs to help SMEs adopt advanced cybersecurity technologies. These programs include government grants and subsidies, cybersecurity voucher programs, public-private partnerships, training and capacity building programs, technology adoption consultancy services, innovation and technology development funds, access to cybersecurity research and development resources, cybersecurity competitions and challenges, international collaboration programs, cybersecurity certification assistance, industry-specific support, and cybersecurity awareness campaigns. These programs provide financial assistance to offset costs associated with implementing AI solutions, enhance skills and knowledge, and provide access to global expertise and insights. SMEs should seek information about these programs from government cybersecurity

agencies, industry associations, and business development organizations, and collaborate with local technology hubs, innovation centers, and industry networks for valuable insights and opportunities for support.

6. FUTURE OUTLOOK

The future of AI-driven cybersecurity for Small and Medium Enterprises (SMEs) in Nigeria presents both challenges and opportunities. Rapid technological change is expected to accelerate, requiring SMEs to adapt quickly to new solutions. The increasing sophistication of cyber threats necessitates the investment in AI-driven solutions that can dynamically adapt to evolving threat landscapes and offer advanced threat detection capabilities. The rising demand for skilled cybersecurity professionals will likely increase, exacerbating the existing skills gap. SMEs may face challenges in recruiting and retaining qualified talent, emphasizing the need for training and upskilling programs. Integrating AI-driven cybersecurity solutions with legacy systems may be challenging, necessitating infrastructure upgrades and compatibility. Opportunities include advances in user-friendly AI solutions, government support and initiatives, collaborative cybersecurity ecosystems, and the rise of tailored AI solutions for SMEs. Governments may increase support and initiatives to help SMEs bolster their cybersecurity capabilities, such as grants, subsidies, and training programs. Collaborative efforts between SMEs, industry partners, and cybersecurity providers may strengthen the overall cybersecurity ecosystem. Tailored AI solutions for SMEs can be cost-effective, scalable, and address specific cybersecurity requirements. Strategic considerations for SMEs include investing in continuous training, embracing collaboration, planning for the agile adoption of emerging technologies, exploring government support programs, and conducting thorough assessments of their existing IT infrastructure to ensure compatibility with AI-driven cybersecurity solutions.

AI-driven cybersecurity for Small and Medium Enterprises (SMEs) is undergoing significant advancements, including AI-powered threat hunting, Zero Trust Security Architecture, Extended Detection and Response (XDR), Behavioral Biometrics, AI in Endpoint Detection and Response (EDR), Explainable AI (XAI), AI for Insider Threat Detection, AI-Enhanced Cloud Security, Adversarial Machine Learning Defense, AI-Driven Automation in Incident Response, AI-Powered Phishing Detection, AI Governance and Ethical AI, and Edge AI for IoT Security. These technologies will enhance threat detection and response, comply with evolving cybersecurity regulations, and make advanced cybersecurity solutions more accessible to SMEs. However, challenges such as adversarial AI attacks, ethical concerns, resource constraints, regulatory complexity, and overreliance on AI without human oversight will need to be addressed. A concerted effort from governments, industry stakeholders, and cybersecurity professionals is needed to ensure responsible and effective integration of AI in SME cybersecurity strategies.

The future of AI-driven cybersecurity in Nigerian SMEs is expected to see increased adoption rates due to growing awareness of cyber threats and the need for advanced security solutions. Advances in AI technology may lead to more affordable and accessible solutions tailored for SMEs, enabling a broader range of businesses to implement robust security measures. Regulatory authorities in Nigeria may place increased emphasis on cybersecurity measures, encouraging SMEs to adopt AI-driven solutions to meet compliance requirements and protect sensitive data. AI cybersecurity solutions may become more customizable to suit the specific needs and resource constraints of SMEs, making it easier for them to implement and manage these technologies effectively. With the growing reliance on cloud services, AI-driven cybersecurity solutions may integrate with cloud security measures, providing comprehensive protection for SMEs operating in cloud environments. Collaboration and partnerships with cybersecurity service providers and technology firms may be increased to access expertise and deploy AI-driven solutions effectively. The Nigerian government may implement initiatives to support SMEs in enhancing their cybersecurity posture, offering

incentives or guidance for the adoption of AI-driven solutions. AI-driven threat hunting may play a more prominent role in proactive threat hunting, while quantum computing threat preparedness may lead to more user-friendly interfaces.

CONCLUSION AND RECOMMENDATIONS

SMEs in Nigeria face several challenges in understanding cybersecurity risks, including limited awareness, a lack of dedicated cybersecurity personnel, resource constraints, and insufficient awareness of available AI solutions. Government initiatives and support programs can help SMEs enhance their cybersecurity measures, while collaboration and information sharing can foster a stronger cybersecurity ecosystem. Advancements in AI technologies offer scalable, adaptive, and cost-effective cybersecurity solutions, and innovations in cybersecurity awareness training empower SME employees to identify and respond to cyber threats. Embracing AI-driven cybersecurity is crucial for sustainable growth, protecting SMEs from financial losses, enhancing business reputation, and ensuring compliance with cybersecurity regulations. Tailored solutions for local challenges, supporting digital transformation, job creation and skill development, and enhancing global competitiveness are some of the benefits of AI-driven cybersecurity. The Nigerian Communications Commission reports that cybercrime costs Nigeria billions of dollars annually, making it crucial for SMEs to adopt AI-driven cybersecurity. Tailored solutions can address specific cyber threats, support digital transformation initiatives, and stimulate job creation and skill development. Furthermore, cybersecurity readiness enhances global competitiveness, allowing SMEs in Nigeria to compete more effectively on the global stage.

Adequate training for local security networks and agencies is crucial and can be effective in offering local intelligence gathering and thereby pass it over to the appropriate military or established intelligence unit where such information is vital and essential. Funding: No funding, grants, or other support were received. Conflict of interest: The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

Aggarwal, D., Sharma, D., & Saxena, A.B. 2023. 'Role of AI in Cyber Security through Anomaly Detection and Predictive Analysis.' *Journal of Informatics Education and Research.* Available at: https://doi.org/10.52783/jier.v3i2.314.

Alfayoumi, S., Eltazi, N., & Elgammal, A. 2023. 'AI-Driven Optimization Approach Based on Genetic Algorithm in Mass Customization Supplying and Manufacturing.' *International Journal of Advanced Computer Science and Applications* 14(11). Available at: https://doi.org/10.14569/ijacsa.

Bada, M., & Nurse, J.R. 2019. 'Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).' *Information & Computer Security* 27(3), pp. 393–410. Available at: https://doi.org/10.1108/ics-07-2018-0080.

Benz, M., & Chatterjee, D. 2020. 'Calculated Risk? A Cybersecurity Evaluation Tool for SMEs.' *Business Horizons* 63(4), pp. 531–40. Available at: https://doi.org/10.1016/j.bushor.2020.03.010.

Bitamuno, P.V. 2023. 'Legal Frameworks for Cybersecurity in Nigeria - Adapting The Fourth Industrial Revolution.' *Advances in Multidisciplinary and Scientific Research Journal*

Publication 2(1), pp. 97–104. Available at: https://doi.org/10.22624/aims/cseansmart2023p12

Bhardwaj, A., & Kaushik, K. 2022. 'Predictive Analytics-Based Cybersecurity Framework for Cloud Infrastructure.' *International Journal of Cloud Applications and Computing* 12(1), pp. 1–20. Available at: https://doi.org/10.4018/ijcac.297106.

Chahal, S. 2023. 'AI-Enhanced Cyber Incident Response and Recovery.' *International Journal of Science and Research (IJSR)* 12(3), pp. 1795–1801. Available at: https://doi.org/10.21275/sr231003163025.

Gaggero, G.B., Girdinio, P., & Marchese, M. 2021. 'Advancements and Research Trends in Microgrids Cybersecurity.' *Applied Sciences* 11(16), pp. 7363. Available at: https://doi.org/10.3390/app11167363.

Gheibi, O., Weyns, D., & Quin, F. 2020. 'Applying Machine Learning in Self-Adaptive Systems.' *ACM Transactions on Autonomous and Adaptive Systems* 15(3), pp. 1–37. Available at: https://doi.org/10.1145/3469440.

International Journal of Marketing, Communication and New Media. 2023. 'Cybersecurity, Privacy, and Data Protection: State of the Art in Iran, Nigeria, Portugal, and the USA.' February. Available at: https://doi.org/10.54663/2182-9306.2023.sn12.1-4.

Joseph, T., Obikaonu, P., Ariolu, C., Nwolisa, C., & Aderohunmu, A. 2021. 'SMEs Intervention Programmes in Nigeria: Evaluating Challenges Facing Implementation.' *Applied Journal of Economics, Management and Social Sciences* 2(1), pp. 16–25. Available at: https://doi.org/10.53790/ajmss.v2i1.10.

Kariuki, P., Ofusori, L.O., & Subramaniam, P.R. 2023. 'Cybersecurity Threats and Vulnerabilities Experienced by Small-Scale African Migrant Traders in Southern Africa.' *Security Journal* June. Available at: https://doi.org/10.1057/s41284-023-00378-1.

Kassar, G. 2023. 'Exploring Cybersecurity Awareness and Resilience of SMEs amid the Sudden Shift to Remote Work during the Coronavirus Pandemic: A Pilot Study.' *ARPHA Conference Abstracts* 6. Available at: https://doi.org/10.3897/aca.6.e107358.

Maurya, R. 2023. 'Analyzing the Role of AI in Cyber Security Threat Detection & Prevention.' *International Journal for Research in Applied Science and Engineering Technology* 11(11), pp. 514–19. Available at: https://doi.org/10.22214/ijraset.2023.56510.

Marotta, A., & Madnick, S.E. 2020. 'Analyzing the Interplay Between Regulatory Compliance and Cybersecurity.' *SSRN Electronic Journal.* Available at: https://doi.org/10.2139/ssrn.3542563.

Rizvi, M. 2023. 'Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention.' *International Journal of Advanced Engineering Research and Science* 10(5), pp. 055–060. Available at: https://doi.org/10.22161/ijaers.105.8.

Thapliyal, A. 2022. 'Importance of Cybersecurity in Financial Services Industry: An Analytical Perspective of Various Security Models.' *International Journal of Early Childhood Special Education* June. Available at: https://doi.org/10.48047/intjecse/v14i2.1074.

Tonhauser, M., & Ristvej, J. 2023. 'Cybersecurity Automation in Countering Cyberattacks.' *Transportation Research Procedia* 74, pp. 1360–65. Available at: https://doi.org/10.1016/j.trpro.2023.11.283.

Ugwuja, V.C., Ekunwe, P.A., & Henri-Ukoha, A. 2020. 'Cyber Risks in Electronic Banking: Exposures and Cybersecurity Preparedness of Women Agro-Entrepreneurs in South- South Region of Nigeria.' *Journal of Business Diversity* 20(3), September. Available at: https://doi.org/10.33423/jbd.v20i3.3087.

Ukwuoma, H.C., Williams, I.S., & Choji, I.D. 2022. 'Digital Economy and Cybersecurity in Nigeria.' *International Journal of Innovation in the Digital Economy* 13(1), pp. 1–11. Available at: https://doi.org/10.4018/ijide.292489.

World Economic Forum. 2019. 'Global Risks Report 2019.' *Computer Fraud & Security* 2019(2), pp. 4–4. Available at: https://doi.org/10.1016/s1361-3723(19)30016-8.